- Environmental LAB

You will build your own lab where we can perform our attacks (any operating system will work).

This lab is essentially a virtual machine that we will use for testing (Kali Linux). Throughout the course, we also create additional virtual vulnerable machines that we can practice our attacks on.

The reason we use virtual machines is because we are not allowed to test our attacks on real-world websites and networks so we create our own environment to do that.

Downloading Virtual Box & Kali Linux

Creating Our First Virtual Machine

Installing Kali Linux Operating System

5 Stages Of A Penetration Test

Navigating Through Kali Linux System

Creating Files & Managing Directories

Network Commands & Sudo Privileges In Kali

1) OPTIONAL: PYTHON 101

Learn Python 3 programming from scratch. This section is not mandatory and is optional for those that want to learn to programming so you are able to build your own ethical hacking tools!

Learn Python Basics

Learn Python Intermediate

Learn Python: Error Handling

Learn Python: File I/O

2) RECONNAISSANCE

You will learn what we call Footprinting (aka Information Gathering). Once we choose our target, our first task is to gain as much information about the target as possible.

What is Information Gathering?

Physical Address Using Whois Tool

What is Web Stealthy Scan

Aggressive Website Technology Discovering on IP Range

Gathering Emails Using theHarvester & Hunterio

How To Download Tools Online

Finding Usernames With Sherlock

Bonus: Email Scraper Tool In Python 3

3) SCANNING

This is where things get real. In this section, we also gather information but we try to gather only technical information (i.e. if they have open ports, if they have a firewall, what software they are running on those open ports, what operating system they have, is it an outdated operating system, etc.).

Theory Behind Scanning

TCP & UDP

Installing Vulnerable Virtual Machine

Netdiscover

Performing First Nmap Scan

Different Nmap Scan Types

Discovering Target Operating System

Detecting Version Of Service Running On An Open Port

Filtering Port Range & Output Of Scan Results

What is a Firewall/IDS?

Using Decoys and Packet Fragmentation

Security Evasion Nmap Options

Python Coding Project - Port Scanner

4) VULNERABILITY ANALYSIS

Use the information that you gathered from scanning (such as software that the target has running on open ports) and with this information, we try to determine whether there are any known vulnerabilities.

Finding First Vulnerability With Nmap Scripts

Manual Vulnerability Analysis & Searchsploit

Nessus Installation

Discovering Vulnerabilities With Nessus

Scanning Windows 7 Machine With Nessus

5) EXPLOITATION & GAINING ACCESS

This is the exciting part of the course. This is where we attack and gain access to the target machines.

Throughout this section, we will be covering many different vulnerabilities and different targets. We perform these attacks on our virtual machines and cover another really important tool for an ethical hacker: Metasploit Framework.

The goal of exploitation is to get on that target machine. This means we must drop a payload on that target machine so we can use it to navigate through their systems, look through their files, execute anything we want, and delete anything we want without the target knowing anything about it.

We will also learn to create our own Viruses and Trojans that we can deliver to the target whether through an email or through a USB.

What is Exploitation?

What is a Vulnerability?

Reverse Shells, Bind Shells

Metasploit Framework Structure

Msfconsole Basic Commands

Our First Exploit - vsftp 2.3.4 Exploitation

Misconfigurations Happen - Bindshell Exploitation

Information Disclosure - Telnet Exploit

Software Vulnerability - Samba Exploitation

Attacking SSH - Bruteforce Attack

Exploitation Challenge - 5 Different Exploits

Explaining Windows 7 Setup

Eternal Blue Attack - Windows 7 Exploitation

DoublePulsar Attack - Windows Exploit

BlueKeep Vulnerability - Windows Exploit

Routersploit

Router Default Credentials

Setting Up Vulnerable Windows 10

Crashing Windows 10 Machine Remotely

Exploiting Windows 10 Machine Remotely

Generating Basic Payload With Msfvenom

Advance Msfvenom Usage

Generating Powershell Payload Using Veil

TheFatRat Payload Creation

Making Our Payload Open An Image

6) POST EXPLOITATION

Post exploitation is what we do on the target machine after we have exploited it.

Once we are on a machine, we can do many things depending on what we want to get out from it. After we do all of the things we wanted, we want to make sure we cover our tracks by deleting any event logs or deleting any evidence that we were ever on that machine.

Post Exploitation Theory

Meterpreter Basic Commands

Elevating Privileges With Different Modules

Creating Persistence On The Target System

Post Exploitation Modules

Python Coding Project - Backdoor

7) WEBSITE PENETRATION TESTING

Another important topic for an Ethical Hacker. In this section, we are mainly targeting websites and their bugs/vulnerabilities. These vulnerabilities can be anything from misconfigurations, SQL Injections (us interacting with the database), Information Disclosures (having access to some information by mistake which shouldn't be out there), Command Injection (directly interacting with

the system through the webpage), XSS (Cross Site Scripting Attack and Injecting Javascript code on the page).

Website Penetration Testing Theory

HTTP Request & Response

Information Gathering & Dirb Tool

Burpsuite Configuration

ShellShock Exploitation

Command Injection Exploitation

Getting Meterpreter Shell With Command Execution

Reflected XSS & Cookie Stealing

Stored XSS

HTML Injection

SQL Injection

CSRF Vulnerability

Hydra Bruteforce Attack

Burpsuite Intruder

Python Coding Project - Login Brute-force + Directory Discovery

8) MAN IN THE MIDDLE

This is an attack that is used inside a network. This allows us to sniff any unencrypted data and see it in plain text. This could also include seeing passwords in plain text for some websites. There are many tools out there that can perform this attack for us. We cover some of the main ones.

Theory - Man In The Middle Attack

Bettercap ARP Spoofing

Ettercap Password Sniffing

9) WIFI CRACKING

Learn how to gain access to a network by cracking its wireless password.

Wireless Cracking Theory

Putting Wireless Card In Monitor Mode

Deauthenticating Devices & Grabbing Password

Aircrack Password Cracking

Hashcat Password Cracking

Bonus Concepts -

- Gaining access to android mobile

- Dark Web